

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*

PROPERTY DESCRIBED AS A RESIDENCE AT
N1683 STATE HIGHWAY 47, NEOPIT, WI 54150

Case No. 23 m 650

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
Title 18, United States Code, Section 2252(a)(3)(A)	Possession of child pornography in Indian Country.

The application is based on these facts:
See Attached Affidavit.

- ☐ Continued on the attached sheet.
☐ Delayed notice of _____ days *(give exact ending date if more than 30 days)*: _____ is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Brian D'Arcy 05/23/23 at 1520
Applicant's signature
Brian D'Arcy, FBI SA
Printed name and title


Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

(specify reliable electronic means).

Date: 5/23/23

City and state: Green Bay, Wisconsin

James R. Sickel
Judge's signature
Magistrate Judge James R. Sickel
Printed name and title



IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN

IN THE MATTER OF THE SEARCH OF
PROPERTY DESCRIBED AS A RESIDENCE
AT N1683 STATE HIGHWAY 47, NEOPIT,
WI 54150

Case No. 23 M 650

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Brian D'Arcy, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as N1683 State Highway 47, Neopit, WI 54150, hereinafter the "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been employed as such since July 2017. Upon graduation from the FBI Academy in Quantico, Virginia, I was assigned to the Milwaukee Division, Green Bay Resident Agency. Since arriving in Green Bay, I have been assigned to work on various criminal violations, to include fraud, child pornography, armed robberies, drug trafficking, and crimes occurring on Native American reservations. I have experience in conducting criminal investigations involving suspects using electronic communications and digital devices to orchestrate criminal activity. I have assisted in the execution of search warrants for the purpose of obtaining documents and digital devices relating to various criminal activity. As a Special Agent of the FBI, I am authorized to investigate

violations of the criminal laws of the United States, and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, information obtained from other law enforcement officers and witnesses, and information provided by the National Center for Missing and Exploited Children (NCMEC). Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts necessary to establish probable cause to believe evidence of violations of Title 18, United States Code, Section 2252(a)(3)(A) is located at the PREMISES, more particularly described in Attachment A of the search warrant.

DEFINITIONS

4. The following non-exhaustive list of definitions applies to this Affidavit and Attachments A and B (collectively referred to as “warrant”):

- a. “Child Pornography” is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8).
- b. “Visual depictions” include data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).
- c. “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
- d. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious

exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

- e. “Computer” means “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” See 18 U.S.C. § 1030(e)(1).
- f. “Computer hardware” consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices), peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).
- g. “Computer passwords and data security devices” consist of information or items designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.
- h. “Internet Service Providers” (ISPs) are commercial organizations, which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage and co-location of computers and other communications equipment. ISPs can offer various means to access the Internet, including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox and the subscriber typically creates a password for the account. By using a

computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

- i. “ISP Records” are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP’s servers and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers’ use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.
- j. “Internet Protocol address” (IP address) refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.
- k. The terms “records,” “documents” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in hand-made form (including writings, drawings, painting), photographic form (including microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including phonograph records, printing, typing) or electrical, electronic or magnetic form (including tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as secure digital (SD) cards, floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- l. “Digital device” includes any electronic system or device capable of storing and/or processing data in digital form, including the following: central processing units; laptop or notebook computers; PDAs; wireless communication devices such as telephone paging devices, beepers and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors and drives intended for removable media; related communications

devices such as modems, cables and connections; storage media such as hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips; and security devices.

- m. "Image" or "copy" refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. "Imaging" or "copying" maintains contents, but attributes may change during the reproduction.
- n. "Compressed file" refers to a file that has been reduced in size through a compression algorithm to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed.
- o. "Log Files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.
- p. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

BACKGROUND ON COMPUTERS/CELLULAR PHONES AND CHILD PORNOGRAPHY AND ONLINE CHILD EXPLOITATION

5. Based upon my knowledge, training, and experience in online child exploitation and child pornography investigations, as well as the experience and training of other law enforcement officers with whom I have had discussions, I have learned the following:

- a. Cellular telephones, Computers, and computer technology have revolutionized the way in which child pornography is produced, distributed, stored and communicated as a commodity and a further tool of online child exploitation.
- b. Individuals can transfer photographs from a camera onto a computer-readable format with a variety of devices, including scanners, memory card readers, or directly from digital devices.
- c. A cellular telephone is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling

communication with other wireless telephones or traditional “land line” telephones. A cellular telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Cellular telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- d. The capability of a cellular telephone to store images in digital form makes the cellular telephone itself an ideal repository for child pornography. As explained further below, the storage capacity of electronic media used in home cellular telephones has increased tremendously within the last several years. These drives can store extreme amounts of visual images at very high resolution.
- e. Modems allow computers to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.
- f. The capability of a computer to store images in digital form makes the computer itself an ideal repository for child pornography. As explained further below, the storage capacity of electronic media used in home computers has increased tremendously within the last several years. These drives can store extreme amounts of visual images at very high resolution.
- g. The Internet, the World Wide Web and other Internet components afford individuals many different and relatively secure and anonymous venues for obtaining, viewing and trading child pornography or for communicating with others to do so or to entice children.
- h. Individuals can use online resources to retrieve, store and share child pornography, including services offered by Internet Portals such as Google, America Online (AOL), Yahoo! and Hotmail, among others. Online services allow a user to set up an account providing e-mail and instant messaging services, as well as electronic storage of electronic files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user’s computer. Even in cases where online

storage is used, evidence of child pornography can be found on the user's computer and cellular devices in most cases.

- i. As is the case with most digital technology, computer communications can be saved or stored on hardware and computer storage media used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. However, digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained for very long periods of time until overwritten by other data.
- j. The interaction between software applications, cellular telephones, and computer operating systems often results in material obtained from the Internet being stored multiple times, and even in different locations, on a cellular telephone or computer hard drive without the user's knowledge. Even if the computer/telephone user is sophisticated and understands this automatic storage of information on his/her computer's hard drive, attempts at deleting the material often fail because the material may be automatically stored multiple times and in multiple locations within the computer media or cellular telephone hard drive. As a result, digital data that may have evidentiary value to this investigation could exist in the user's computer media despite, and long after, attempts at deleting it. A thorough search of this media could uncover evidence of receipt, distribution, and or possession of child pornography.
- k. Data that exists on a computer or cellular telephone is particularly resilient to deletion. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear, rather, the data remains on the hard drive until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive not allocated to an active file or unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a computer or cellular telephone's

operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed and more on a particular user’s operating system, storage capacity, and computer habits.

1. I know that persons who collect, receive, and distribute child pornography often access child pornography from multiple devices. Therefore, child pornography is often cached or stored on multiple electronic devices. These devices include cellular telephones, personal computers, tablets, and other electronic storage devices.

BACKGROUND ON DIGITAL EVIDENCE ASSESSMENT PROCESS IN CHILD PORNOGRAPHY AND CHILD EXPLOITATION INVESTIGATIONS

6. Based upon my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know segregating information before commencement of the review of digital evidence by the examining agent is inconsistent with the evidence assessment process in child pornography and online child exploitation investigations. This is true in part because the items to be searched will not only contain child pornography but also will contain the identity of the user/possessor of the child pornography as well as evidence as to the programs and software used to obtain the child pornography, which may be located throughout the areas to be searched.

7. As further described in Attachment B, this warrant seeks permission to locate not only electronic files that might serve as direct evidence of the crimes described in the warrant, but also for evidence that establishes how computers and digital devices were used, the purpose of their use, and who used them. Additionally, the warrant seeks information about the possible location of other evidence.

8. As described above and in Attachment B, this application seeks permission to search and seize certain records found on the PREMISES, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive, or other electronic media. Some of these electronic records might take the form of files, documents, and other user-generated data. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

9. Although some of the records called for by this affidavit might be found in the form of user-generated documents (such as word processor, picture and movie files), computer hard drives can contain other forms of electronic evidence that are not user-generated. In particular, a computer hard drive may contain records of how a computer has been used, the purposes for which it was used and who has used these records, as described further in the attachments. For instance, based upon my knowledge, training and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know the following:

- a. Data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph deleted from a word processing file).
- b. Virtual memory paging systems can leave traces of information on the hard drive showing what tasks and processes the computer were recently in use.
- c. Web browsers, e-mail programs, and chat programs store configuration information on the hard drive that can reveal information such as online nicknames and passwords.
- d. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices and the times the computer was in use.
- e. Computer file systems can record information about the dates files were created and the sequence in which they were created. This information may be evidence of a crime or indicate the existence and location of evidence in other locations on the hard drive.

10. Further, in finding evidence of how a computer has been used, the purposes for which it was used and who has used it, sometimes it is necessary to establish a particular thing is not present on a hard drive or a particular person (in the case of a multi-user computer) was not a user of the computer during the time(s) of the criminal activity. For instance, based upon my knowledge, training and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know when a computer has more than one user, files can contain information indicating the dates and times that files were created as well as the sequence in which they were created, and, for example, by reviewing the Index.dat files (a system file that keeps track of historical activity conducted in the Internet Explorer application), whether a user accessed other information close in time to the file creation dates, times and sequences so as to establish user identity and exclude others from computer usage during times related to the criminal activity.

11. Evidence of how a digital device has been used, what it has been used for and who has used it, may be the absence of particular data on a digital device and requires analysis of the digital device as a whole to demonstrate the absence of particular data. Evidence of the absence of particular data on a digital device is not segregable from the digital device.

12. The types of evidence described above may be direct evidence of a crime, indirect evidence of a crime indicating the location of evidence or a space where evidence was once located, contextual evidence identifying a computer user and contextual evidence excluding a computer user. All of these types of evidence may indicate ownership, knowledge and intent.

13. This type of evidence is not “data” that can be segregated, that is, this type of data cannot be abstractly reviewed and filtered by a seizing or imaging agent and then transmitted to

investigators. Rather, evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves and how computers are used. Therefore, contextual information is necessary to understand how the evidence described in Attachment B also falls within the scope of the warrant.

SEARCH METHODOLOGY TO BE EMPLOYED

14. As noted within this search warrant, it would be extremely difficult, if not impossible to conduct a thorough on-site review of all of the potential evidence in this case. Given these constraints, the search methodology to be employed is as follows:

- a. All computers, computer hardware, and any form of electronic storage that could contain evidence described in this warrant will be seized for an off-site search for evidence described in the attachments of this warrant. It is anticipated mirror copies or images of such evidence will be made if the failure to do so could otherwise potentially alter the original evidence.
- b. Consistent with the information provided within this affidavit, contextual information necessary to understand the evidence, to identify the user/possessor of the child pornography, and to establish admissibility of the evidence in subsequent legal proceedings will also be sought by investigative agents.
- c. Additional techniques to be employed in analyzing the seized items will include; (1) surveying various file directories and the individual files they contain; (2) opening files to determine their contents; (3) scanning storage areas; (4) performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in this affidavit and its attachments; and (5) performing any other data analysis techniques that may be necessary to locate and retrieve the evidence described in this affidavit and its attachments.
- d. Because it is expected computers, computer hardware and any form of electronic storage media may constitute, (1) instrumentality of the offense, (2) fruit of criminal activity, (3) contraband, or (4) evidence otherwise unlawfully possessed, it is anticipated such evidence will not be returned to the owner and will be either forfeited or ultimately destroyed in accordance with the law at the conclusion of the case.

- e. Because of the large storage capacity as well as the possibility of hidden data within the computers, computer hardware and any form of electronic storage media, it is anticipated there will be no way to ensure contraband-free evidence could be returned to the user/possessor of the computer, computer hardware or any form of electronic storage media, without first wiping such evidence clean. Wiping the original evidence clean would mean the original evidence would be destroyed and thus, would be detrimental to the investigation and prosecution of this case.
- f. Further, because investigators cannot anticipate all potential defenses to the offenses in this affidavit, and as such, cannot anticipate the significance of the evidence lawfully seized pursuant to this warrant, it is requested that all seized evidence be retained by law enforcement until the conclusion of legal proceedings or until other order of the court.
- g. If after careful inspection investigators determine such computers, computer hardware and electronic storage media do not contain, (1) instrumentality of the offense, (2) fruit of criminal activity, (3) contraband, (4) evidence otherwise unlawfully possessed, or (5) evidence of the person who committed the offense and under what circumstances the offense was committed, then such items seized will be returned.

**CHARACTERISTICS OF INDIVIDUALS INVOLVED IN THE DISTRIBUTION OF
CHILD PORNOGRAPHY**

15. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals involved in the possession and distribution of child pornography. Those who possess and distribute child pornography:

- a. May receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, cartoons, or other visual media; or from literature describing such activity.
- b. May collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media.

Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

- c. Often possess and maintain their “hard copies” of child pornographic material that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- d. Often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the individual’s residence, to enable the collector to view the collection, which is valued highly.
- e. May correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- f. Prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

PROBABLE CAUSE

16. On or about November 2021, the Green Bay Resident Agency of the Federal Bureau of Investigation (FBI) received National Center for Missing & Exploited Children (NCMEC) CyberTipline Report 100227706 and supporting documentation from the Wisconsin Department of Justice, Division of Criminal Investigation (DCI). According to the CyberTipline Report, Microsoft Corporation reported an incident of possible child pornography possession, manufacture, and/or distribution through the BingImage platform. According to the report,

“BingImage (referred to as Visual Search) is a service that provides similar images to an image provided by the user. This image can be provided either via upload or as a URL. The DateTime provided indicates the time at which the image was received and evaluated by the BingImage service. The report listed the incident times and IP addresses for two uploaded images as follows:

- a. File name: 10f73da5-e274-4ac9-b0a8-4f4cdd259d13.jpg; IP Address: 45.53.21.159; Date/Time: 09-04-2021 15:39:23 UTC.
- b. File name: 7bd2fcc2-8056-4221-a903-c6474f00dc75.jpg; IP Address: 45.53.21.159; Date/Time: 09-04-2021 15:45:45 UTC.

17. The image with file name 10f73da5-e274-4ac9-b0a8-4f4cdd259d13.jpg depicts a nude prepubescent female sitting on a bed with her legs crossed underneath her. The female's breasts and vagina are lasciviously displayed. The image with file name 7bd2fcc2-8056-4221-a903-c6474f00dc75.jpg depicts a prepubescent female standing between a toilet and a washing machine wearing black lingerie bottoms. The female's breasts are exposed and her vagina is lasciviously displayed.

18. The CyberTipline report listed the Internet service provider (ISP) for the IP address as Frontier Communications. On November 19, 2021, DCI issued an administrative subpoena to Frontier Communications of America, Inc. requesting subscriber information for the IP addresses and times listed in the CyberTipline report. On November 19, 2021, Frontier provided a response to the subpoena with the following information:

- a. Username: jmp2; Email Address: jmp2@frontiernet.net; Account Name: Jerry Pocan; Account Address: N01683 Hwy 47, Keshena, WI; Telephone Number: 715-799-3716; Billing Address: P.O. Box 512, Keshena, WI 54135-0512.

19. On March 7, 2023, the Green Bay Resident Agency received NCMEC CyberTipline Report 137328055 and supporting documentation from the Wisconsin Department

of Justice, Division of Criminal Investigation (DCI). According to the CyberTipline Report, Microsoft Corporation reported an incident of possible child pornography possession, manufacture, and/or distribution through the BingImage platform. The report listed the incident time and IP address for one uploaded image as follows:

- a. File name: 785b0eaf-b79b-462b-a9d5-b8e7cc543564.jpg; IP Address: 50.50.143.52; Date/Time: 10-22-2022 13:57:23 UTC.

20. The image depicts a nude prepubescent female laying on her back on what appears to be a table. The female is using her hands to expose her vagina to the camera.

21. The CyberTipline report listed the Internet service provider (ISP) for the IP address as Frontier Communications. On February 10, 2023, DCI issued an administrative subpoena to Frontier Communications of America, Inc. requesting subscriber information for the IP address and time listed in the CyberTipline report. On February 10, 2023, Frontier provided a response to the subpoena with the following information:

- a. Customer Name: Jerry Pocan; Telephone Number: 715-799-3716; MAC Address: a0:68:7e:31:37:e1; Email Address: jmp2@frontiernet.net; Connect Date: 07/10/1995; Account Address: N01683 Hwy 47, Keshena, WI; Mailing Address: P.O. Box 512, Keshena, WI.

22. On May 11, 2023, the Green Bay Resident Agency received NCMEC CyberTipline Report 159572581 and supporting documentation from the Wisconsin Department of Justice, Division of Criminal Investigation (DCI). According to the CyberTipline Report, Microsoft Corporation reported an incident of possible child pornography possession, manufacture, and/or distribution through the BingImage platform. The report listed the incident times and IP addresses for four uploaded images as follows:

- a. File name: 864e226b-9d3c-4b52-a4a2-fb09f877a33e.jpg; IP Address: 65.37.117.49; Date/Time: 01-14-2023 17:31:45 UTC.
- b. File name: 5f62c806-4a40-42e4-973a-b86a07d09540.jpg; IP Address: 65.37.117.49; Date/Time: 01-14-2023 17:30:45 UTC.
- c. File name: 1fd9a2ad-d3c0-4afa-bfb0-5d636160ad75.jpg; IP Address: 65.37.117.49; Date/Time: 01-14-2023 17:30:55 UTC.
- d. File name: 140055ad-f801-44bb-849b-58f47a072227.jpg; IP Address: 65.37.117.49; Date/Time: 01-14-2023 17:30:17 UTC.

23. The images with file names 864e226b-9d3c-4b52-a4a2-fb09f877a33e.jpg, 5f62c806-4a40-42e4-973a-b86a07d09540.jpg, 1fd9a2ad-d3c0-4afa-bfb0-5d636160ad75.jpg, and 140055ad-f801-44bb-849b-58f47a072227.jpg appear to be the same image. Additionally, the images share the same MD5 Hash of ca983b4b1d4ab90e4dcc3f932773341f. In my training and experience, I am aware that hash values can be thought of as fingerprints for files. The contents of a file are processed through a cryptographic algorithm and a unique numerical value (the hash value) is produced, which identifies the contents of the file. If the contents of the file are modified in any way, the value of the hash will also change. Two algorithms are currently widely used to produce hash values: the MD5 and SHA1 algorithms. Given this information, the images are likely the same.

24. The image depicts a montage containing nine separate photos of a prepubescent female. The female is lying on a bed with her pajama bottoms or shorts pulled down and her legs spread, while using her hands to expose her vagina and anus to the camera in various positions.

25. The CyberTipline report listed the Internet service provider (ISP) for the IP address as Frontier Communications. On May 9, 2023, DCI issued an administrative subpoena to Frontier Communications of America, Inc. requesting subscriber information for the IP address provided in the CyberTipline report between 17:30:17 UTC and 17:30:55 UTC on 01/14/2023. On May 9, 2023, Frontier provided a response to the subpoena with the following information:

- a. Account Name: Jerry Pocan; Username: jmp2; Account Address: P.O. Box 512, Keshena, WI 54135-0512; Billing Address: N01683 Hwy 47, Keshena, WI 54135; Telephone Number: 715/799-3716; Email Address: jmp2@frontiernet.net; ISP Activated: 02-07-2000 to present; Service Type: Residence – broadband and digital phone.

26. Following the receipt of the NCMEC CyberTipline reports, the MD5 Hash Values associated with the reported images were submitted to NCMEC for an initial hash value comparison report. As previously mentioned, hash values essentially act as fingerprints for files. These “fingerprints” can be used by NCMEC to compare submitted hash values to the hash values of known child pornography images or videos that have been previously identified by NCMEC. After submitting the MD5 hash values associated with the CyberTipline reports, NCMEC reported that the hash values were unrecognized. According to the report, this means that, “These exact hash values are associated with images/videos that have not yet been submitted to NCMEC’s Child Recognition and Identification System.”

27. After reviewing the above-mentioned reports provided by NCMEC, I requested any reports involving Jerry Pocan or N1683 State Highway 47 from the Menominee Tribal Police Department (METPD). According to the METPD reporting system, on February 21, 2021, a call for service (CFS) was initiated at N1683 State Highway 47, Neopit, WI 54150. The reporter was listed as Jerry Pocan, who stated that he believed there was a car stuck in his driveway and that he saw a female walk up his driveway, who may have taken something from his yard. METPD Officer Paige Lehman made contact with the driver of the vehicle, who was stuck in Pocan’s driveway after trying to turn around. The driver went up to Pocan’s residence and grabbed a broken shovel. Officer Lehman then made contact with Pocan in the garage of his residence to inform him of the situation.

28. In addition to this report, another call for service involving Pocan on April 30, 2023 was also located. According to the call for service report, Crystal Pocan requested a welfare check on Jerry Pocan. Crystal said that she normally spoke with Jerry on a daily basis and had not heard from him in over four weeks. At approximately 2:35 PM on April 30, 2023, METPD Officer Chelsea Holstrom made contact with Jerry at N1683 State Highway 47, Neopit, WI 54150, who said that he was fine.

29. According to the subscriber information provided by Frontier Communications in response to the administrative subpoenas submitted by DCI, the subscriber address was listed as N01683 Hwy 47, Keshena, WI. Based on a review of Tribal records and Wisconsin Driver's license information provided for Jerry Pocan, I believe the "0" contained in the user address (N01683) was incorrectly added. According to Wisconsin driver's license information provided for Jerry Pocan, Pocan's listed address is 1683 State Highway 47, Keshena, WI 54135. Additionally, METPD records list Pocan's residence as N1683 State Highway 47, Neopit, WI 54150. I also reviewed the Menominee County & Reservation Fire Number & Road Directory, which lists N1683 as part of the Midway Addition of the Reservation. The N1683 parcel is depicted between Crowe Settlement Road, located to the south of the parcel on State Highway 47, and Midway Road, located to the North of the parcel on State Highway 47. N1683 is situated to the Southwest of State Highway 47, as the parcel appears on Google Maps satellite imagery. Based on a discussion with METPD Detective Joshua Lawe, I am aware that the location of N1683 is considered a part of the village of Neopit on the Menominee Indian Reservation, which is why Tribal records have the address listed as N1683 State Highway 47, Neopit, WI 54150. Given this

information, the PREMISES will be referred to as N1683 State Highway 47, Neopit, WI 54150 for the purposes of this affidavit.

30. On May 15, 2023, I conducted an open-source records search of telephone number 715-799-3716, which was included in the subscriber information provided by Frontier Communications. According to the most recent records, telephone number 715-799-3716 was listed under the name Jerry M. Pocan with an address of P.O. Box 512, Keshena, WI 54135-0512. The phone number is listed as an active landline operated by Frontier Communications. I also conducted an open-source records search of the email address jmp2@frontiernet.net, which was included in the subscriber information provided by Frontier Communications. According to the search results, the email address was listed to Jerry Pocan and P.O. Box 512, Keshena, WI 54135-0512.

31. As described in this affidavit, the CyberTipline reports provided by NCMEC detail the use of the BingImage platform to upload images of child pornography. According to the report, “BingImage (referred to as Visual Search) is a service that provides similar images to an image provided by the user. This image can be provided either via upload or as a URL. The DateTime provided indicates the time at which the image was received and evaluated by the BingImage service.” For each upload event, DCI submitted administrative subpoenas to Frontier Communications for the subscriber information associated with the IP address and time at which the image was uploaded through the BingImage platform. The subscriber information provided by Frontier for each of the upload events resolved to the same account address or billing address and account name: N01683 Hwy 47, Keshena, WI and Jerry Pocan. Based on this information, I believe that an individual located at the PREMISES uploaded multiple images of child pornography to the

BingImage platform to search for similar images. Given this information and the information contained in this affidavit, I believe that evidence of violations of Title 18, United States Code, Section 2252(a)(3)(A) will likely be located at the PREMISES.

BIOMETRIC ACCESS TO DEVICES

32. This warrant permits law enforcement to compel Jerry Pocan to unlock any devices requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

33. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

34. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his/her fingerprints. For example, Apple offers a feature called “Touch ID” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referring to the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

35. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his/her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his/her face, and the device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

36. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his/her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his/her iris/es by holding the device in front of his/her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's iris/es. The device can then be unlocked if the infrared-sensitive camera detects the registered iris/es. Iris-recognition features found on other devices produced by other manufacturers have different names but operate similarly to Windows Hello.

37. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's content. This is particularly true when the user of a device is engaged in criminal activity and thus has a heightened concern about securing the content of a device.

38. As discussed herein, your affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock any device subject to search under this warrant is currently not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device, making the use of biometric features necessary to the execution of the search authorized by this warrant.

39. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

40. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of Pocan to the fingerprint scanner of the device/s found at the

PREMISES; (2) hold the devices found at the PREMISES in front of the face of Pocan and activate the facial recognition feature; and or (3) hold the device/s found at the PREMISES in front of the face of Pocan and activate the iris recognition feature, for the purpose of attempting to unlock the device/s in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel Pocan to state or otherwise provide the passcode or password or any other means that may be used to unlock or access the device. Moreover, the proposed warrant does not authorize law enforcement to compel Pocan to identify the specific biometric characteristics (including the unique finger/s or other physical feature/s) that may be used to unlock or access the device.

41. Based on my training and experience, I know that a person's "identifying physical characteristic[s]" are not testimonial and thus fall "outside [the] protection" of the Fifth Amendment. *Gilbert v. California*, 388 U.S. 263, 267 (1967). The privilege against self-incrimination is not violated by an order compelling a person to submit to photographing and measurements or to provide fingerprints, writing samples, or voice exemplars. See, e.g., *United States v. Dionisio*, 410 U.S. 1, 7 (1973); *California v. Byers*, 402 U.S. 424, 431-32 (1971); *Gilbert*, 388 U.S. at 266-67; *Schmerber v. California*, 384 U.S. 757, 763-64 & n.8 (1966); see also *In the Matter of the Search of [Redacted] Washington, District of Columbia*, 317 F.Supp.3d 523, 540 (D.D.C. 2018) (search warrant authorizing compelled use of biometric feature to unlock devices did not violate Fourth or Fifth Amendments); and *In the Matter of the Search of: a White Google Pixel 3XL Cellphone in a Black Incipio Case*, 398 F.Supp.3d 785, 794 n.8 (D. Idaho 2019) (search warrant authorizing compelled use of biometric feature to unlock devices did not violate Fifth Amendment because it does not require suspect to provide any testimonial evidence; court also

found that such a “search and seizure” would likewise comport with the Fourth Amendment’s reasonableness requirement); but cf. United States v. Warrant, No. 19-mj-71283, 2019 WL 4047615, at *2-3 (N.D. Cal. Aug. 26, 2019) (search warrant compelling application of biometric features authorized if, among other things, law enforcement personnel have information that compelled individual has ability to unlock device as a foregone conclusion).

CONCLUSION

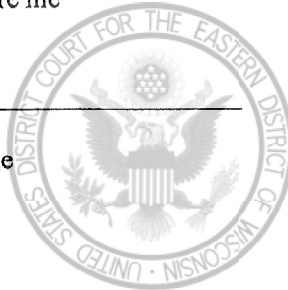
42. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

B. M. D'Arcy 05/23/23 at 1520
BRIAN M. D'ARCY
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on May 22, 2023:

HON. JAMES R. SICKEL
United States Magistrate Judge



ATTACHMENT A

Property to be searched

The property to be searched is N1683 State Highway 47, Neopit, Wisconsin, 54150, further described as a single-level residence with a walk-out basement, tan/beige siding, a green metal roof, and an attached two-car garage. At the entrance of the driveway leading to the residence is a red and white fire number sign with the numerals N1683.

The premises to be searched include any persons on the premises of N1683 State Highway 47, any outbuildings located on the property, and Pocan's vehicles, a 1997 Cadillac Deville, license plate #209VUV, and a 1998 Ford truck, license plate #414HYE.

ATTACHMENT B
Property to be seized

All records relating to violations of Title 18, United States Code, Section 2252(a)(3)(A), those violations involving the PREMISES or Jerry Pocan, and occurring after September 3, 2021, including:

1. Computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic

messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

9. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

11. Any and all cameras, film, videotapes or other photographic equipment.

12. Any and all visual depictions of minors.

13. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

14. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

15. For any computer, computer hard drive, or other physical object upon which electronic information can be recorded (hereinafter, computer) that is called for by this warrant, or that might contain things otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer;
- f. evidence of the times the computer was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the computer;
- h. documentation and manuals that may be necessary to access the computer or to conduct a forensic examination of the computer;
- i. contextual information necessary to understand the evidence described in this attachment.

16. Routers, modems, and network equipment used to connect computers to the Internet.

17. During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to compel Jerry Pocan to provide biometric features, including pressing fingers (including thumbs) against and or putting a face

before a sensor, or any other security feature requiring biometric recognition, of:

- a. any of the devices found at the PREMISES, and
- b. where the device/s are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense/s as described in the search warrant affidavit and warrant attachments

for the purpose of attempting to unlock the device's security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to request Pocan state or otherwise provide the passcode or password or any other means that may be used to unlock or access the device/s, including by identifying the specific biometric characteristics (including the unique finger/s or other physical feature/s) that may be used to unlock or access the device/s.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.